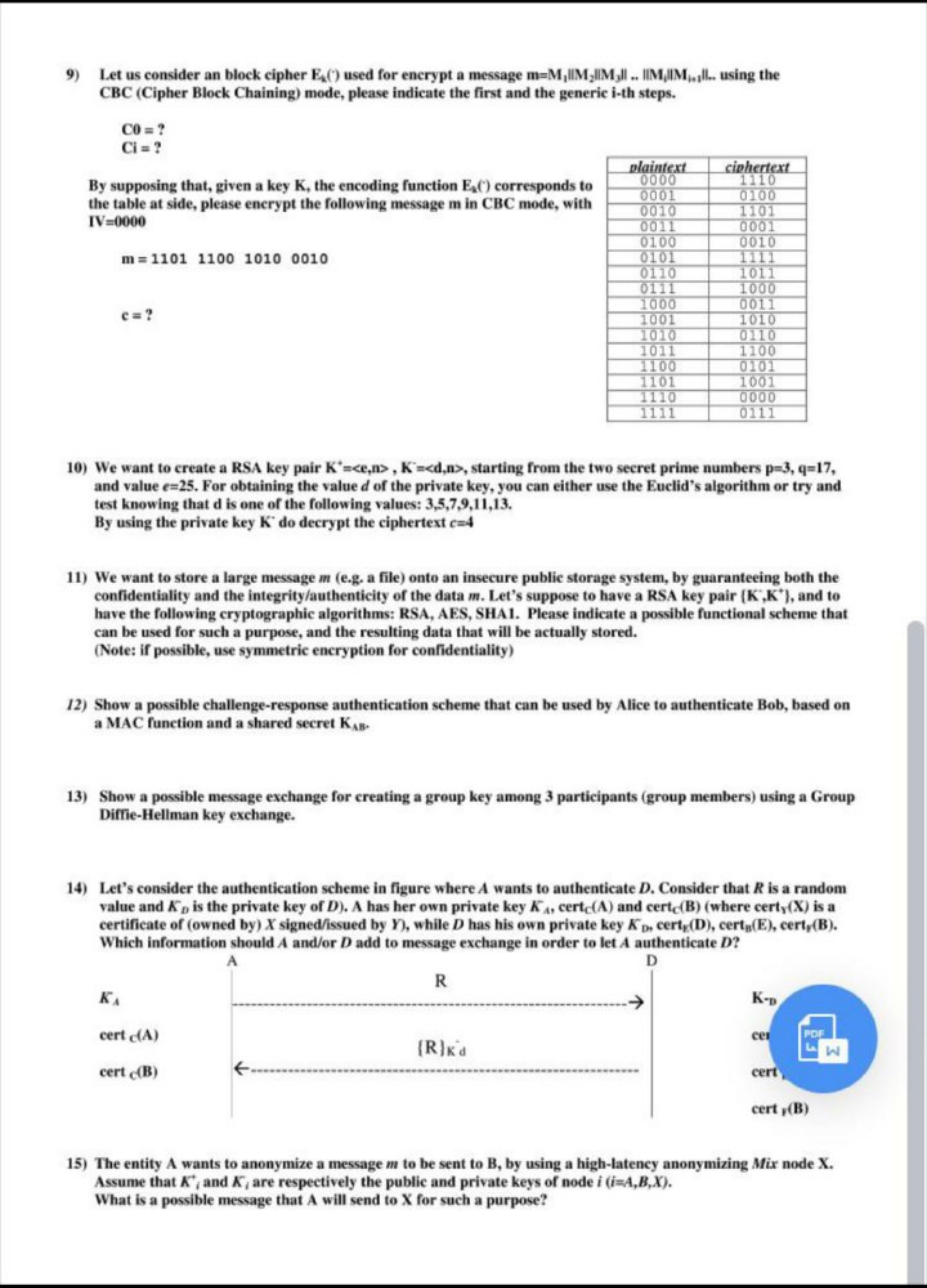


9) Let us consider an block cipher $E_k(\cdot)$ used for encrypt a message $m = M_1 || M_2 || M_3 || \ldots || M_i || M_{i+1} || \ldots$ using the CBC (Cipher Block Chaining) mode, please indicate the first and the generic i-th steps.

C0 = ?
Ci = ?

By supposing that, given a key K, the encoding function $E_k(\cdot)$ corresponds to the table at side, please encrypt the following message m in CBC mode, with IV=0000

m = 1101 1100 1010 0010

c = ?

plaintext	*ciphertext*
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

10) We want to create a RSA key pair $K^+ = <e,n>$, $K^- = <d,n>$, starting from the two secret prime numbers p=3, q=17, and value *e*=25. For obtaining the value *d* of the private key, you can either use the Euclid's algorithm or try and test knowing that d is one of the following values: 3,5,7,9,11,13.
By using the private key K^- do decrypt the ciphertext *c*=4

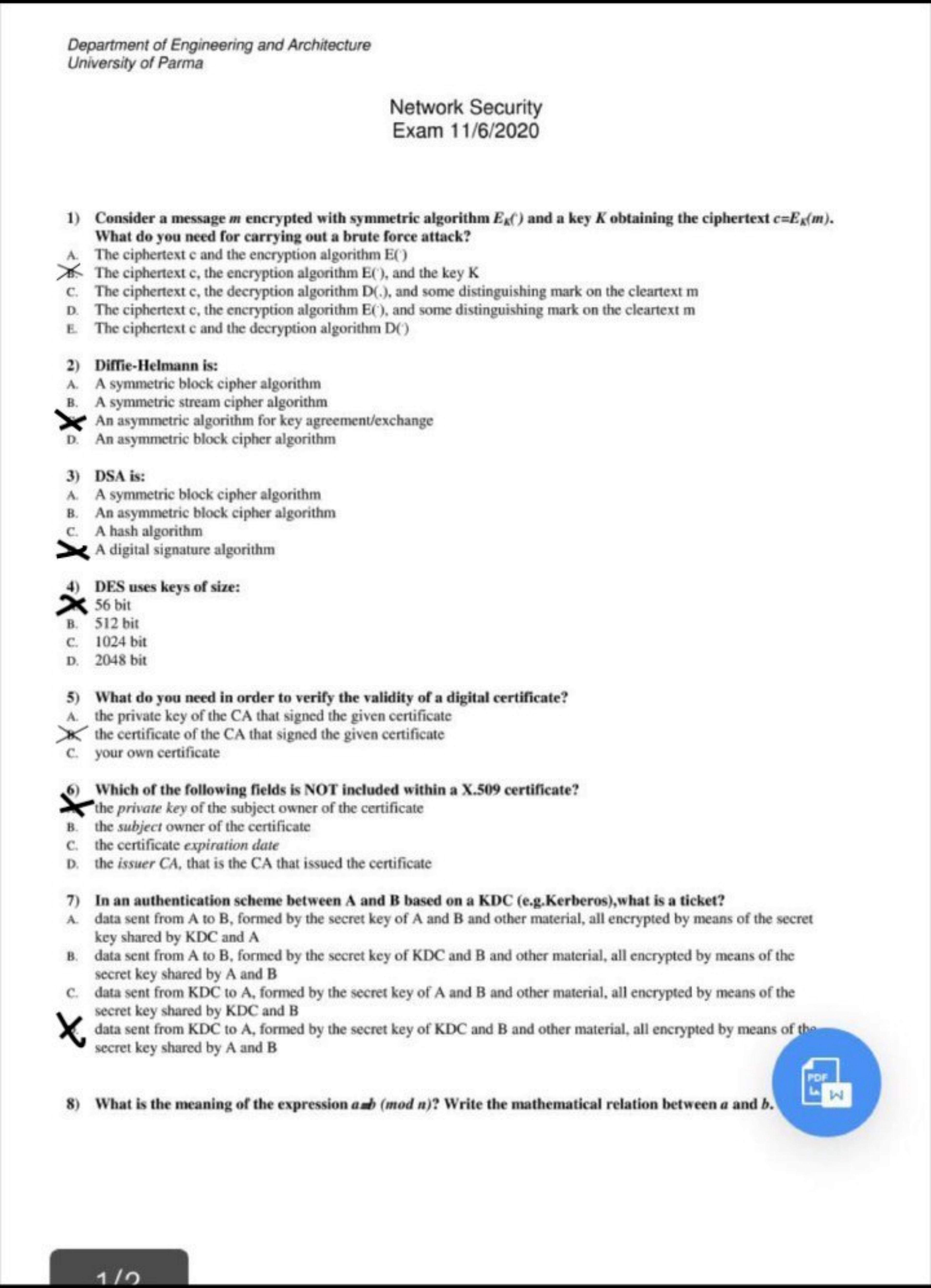
11) We want to store a large message *m* (e.g. a file) onto an insecure public storage system, by guaranteeing both the confidentiality and the integrity/authenticity of the data *m*. Let's suppose to have a RSA key pair $\{K^-, K^+\}$, and to have the following cryptographic algorithms: RSA, AES, SHA1. Please indicate a possible functional scheme that can be used for such a purpose, and the resulting data that will be actually stored.
(Note: if possible, use symmetric encryption for confidentiality)

12) Show a possible challenge-response authentication scheme that can be used by Alice to authenticate Bob, based on a MAC function and a shared secret K_{AB}.

13) Show a possible message exchange for creating a group key among 3 participants (group members) using a Group Diffie-Hellman key exchange.

14) Let's consider the authentication scheme in figure where *A* wants to authenticate *D*. Consider that *R* is a random value and K^-_D is the private key of *D*). A has her own private key K^-_A, $cert_C(A)$ and $cert_C(B)$ (where $cert_Y(X)$ is a certificate of (owned by) *X* signed/issued by *Y*), while *D* has his own private key K^-_D, $cert_E(D)$, $cert_B(E)$, $cert_F(B)$.
Which information should *A* and/or *D* add to message exchange in order to let *A* authenticate *D*?

15) The entity A wants to anonymize a message *m* to be sent to B, by using a high-latency anonymizing *Mix* node X. Assume that K^+_i and K^-_i are respectively the public and private keys of node *i* (*i*=*A*,*B*,*X*).
What is a possible message that A will send to X for such a purpose?



Department of Engineering and Architecture
University of Parma

Network Security
Exam 11/6/2020

1) **Consider a message *m* encrypted with symmetric algorithm $E_K()$ and a key *K* obtaining the ciphertext $c=E_K(m)$. What do you need for carrying out a brute force attack?**

A. The ciphertext c and the encryption algorithm E()
[✓ B. The ciphertext c, the encryption algorithm E(), and the key K]
C. The ciphertext c, the decryption algorithm D(.), and some distinguishing mark on the cleartext m
D. The ciphertext c, the encryption algorithm E(), and some distinguishing mark on the cleartext m
E. The ciphertext c and the decryption algorithm D()

2) **Diffie-Helmann is:**

A. A symmetric block cipher algorithm
B. A symmetric stream cipher algorithm
[✓ C. An asymmetric algorithm for key agreement/exchange]
D. An asymmetric block cipher algorithm

3) **DSA is:**

A. A symmetric block cipher algorithm
B. An asymmetric block cipher algorithm
C. A hash algorithm
[✓ D. A digital signature algorithm]

4) **DES uses keys of size:**

[✓ A. 56 bit]
B. 512 bit
C. 1024 bit
D. 2048 bit

5) **What do you need in order to verify the validity of a digital certificate?**

A. the private key of the CA that signed the given certificate
[✓ B. the certificate of the CA that signed the given certificate]
C. your own certificate

6) **Which of the following fields is NOT included within a X.509 certificate?**

[✓ A. the *private key* of the subject owner of the certificate]
B. the *subject* owner of the certificate
C. the certificate *expiration date*
D. the *issuer CA*, that is the CA that issued the certificate

7) **In an authentication scheme between A and B based on a KDC (e.g.Kerberos),what is a ticket?**

A. data sent from A to B, formed by the secret key of A and B and other material, all encrypted by means of the secret key shared by KDC and A
B. data sent from A to B, formed by the secret key of KDC and B and other material, all encrypted by means of the secret key shared by A and B
C. data sent from KDC to A, formed by the secret key of A and B and other material, all encrypted by means of the secret key shared by KDC and B
[✓ D. data sent from KDC to A, formed by the secret key of KDC and B and other material, all encrypted by means of the secret key shared by A and B]

8) **What is the meaning of the expression $a \equiv b \pmod{n}$? Write the mathematical relation between *a* and *b*.**